

REMARKS

The Applicants have studied the Office Action dated October 1, 2004 and have made amendments to the claims to distinctly claim and particularly point out the subject matter which the Applicants regard as the invention. No new matter has been added. It is submitted that the application, as amended, is in condition for allowance. Claims 2, 10 and 17 have been cancelled without prejudice or disclaimer. Claims 18-22 have been added. By virtue of this amendment, claims 1, 3-9, 11-16, and 18-22 are pending. Reconsideration and allowance of the pending claims in view of the above amendments and the following remarks is respectfully requested.

In the Office Action, the Examiner:

- (1-2) noted claims 1-16 are pending in the application; and
- (3) rejected claim 1 under 35 U.S.C. § 102(b) as being anticipated by Stefik (U.S. 5,715,403); and
- (4) rejected claims 2-16 under 35 U.S.C. § 103(a) as being unpatentable over Stefik (U.S. 5,715,403) in view of Yoshiura et al. (US 6,131,162).

Overview of the Present Invention

The present invention is directed to a method, system and computer readable medium for updating previously stored usage conditions to allow additional copies of previously received encrypted digital content to be made on a computer readable medium such as recordable CDs, DVDs, ZipDisksTM, tape, Flash memory, and RAM. The present invention overcomes the inability to purchase another copy of content which has been previously downloaded to the end user system. Stated differently, the present invention overcomes the time consuming problem of re-downloading content when an end user has a license for the content and desires to purchase another copy of the content. Moreover, many times in the prior art system not only must the content be re-downloaded in order to make a copy but the any additional data or meta data such as lyrics and artwork many times is downloaded with the content as well. The present invention overcomes this problem by permitting an end user to update usage conditions

SOM920000016US1

8

09/711,747

in lieu of downloading digital rights management protected content.

During the creation of the encrypted digital content, in a section entitled "Secure Container Packing" process, as described in the application as originally filed, the hash values for the secure container parts are created. The hash value of the Content 113 including the track information, metadata such as artwork, etc. is placed in the Offer SC(s) 641 that is received by the End User Device(s) 105 from the Electronic Digital Content Store(s) 103. When an end user makes a purchase, the hash value is placed in the Transaction SC(s) 640 that is sent to the End User Device(s) 105. The Helper Application 109 on the End User Device(s) 105 stores the hash value in the local license database 197 for the specific Content 113. When a second copy (or additional copy) of the identical Content 113 is purchased using the flow of the Offer SC(s) 641 and Transaction SC(s) 640 as described in FIG. 6, the Player Application 196 searches the local license database 197 for the Content 113. If the Content 113 already exists in the local database 113, then a comparison is made of the hash from the new Transaction SC(s) received during the end users' request for an additional license is received on the End User Device(s) 109. If hash values are identical, then another download of the Content from the Content Hosting Site(s) 111 can be avoided because the Content 113 is exactly the same content as previously downloaded. On the other hand, if the hash values are different, then the content requested must be downloaded from the Content Hosting Site(s) since something, i.e., the content itself, the artwork, or other metadata relevant to the Content 113 has changed. The advantage of this invention is that consumers who purchase an additional copy of content that they already have downloaded do not have to go through the download of that content. The Usage Rights 519 that they currently have will be updated.

In order to more clearly point of the feature of comparing previously stored hash vales of electronics digital content with a hash value received in response to a request to copy previously received electronic digital content, and then updating the usage conditions associated with the previously received digital content, the following language has been added to the independent claims, i.e., claims 1, 7, 9, 15, and 18 as follows:

SOM920000016US1

9

09/711,747

- claims 1, 9, and 18
 - receiving from an electronic store, a hash value associated with the request to create the copy of previously received encrypted digital content;
 - comparing the hash value received from the electronic store with a previously stored hash value corresponding to the previously received encrypted digital content;
 - updating the usage conditions associated with the previously received encrypted digital content to permit the at least one additional copy, in response to the hash value received from the electronic store matching the previously stored hash value; and
 - creating at least one additional copy onto a computer readable medium of the previously received encrypted digital content, if the at least one additional copy has been authorized in the usage conditions associated with the previously received encrypted digital content and without the need to re-receive the encrypted digital content being copied.
- claims 7 and 15
 - determining if the first hash value received is identical to the second hash value and in response to the first hash and the second hash value being identical, then authorizing the creating additional copies onto at least one computer readable medium by updating the associated usage conditions and without the need to re-receive the encrypted digital content being copied.

Support for this amendment is found on pages 153-154 and figures 1, 6, 10 and 20. No new matter has been added.

(3) Rejection under 35 U.S.C. §102(b) over Stefik

As noted above, the Examiner rejected claim 1 under 35 U.S.C. § 102(b) as being anticipated by Stefik (U.S. 5,715,403). Independent claim 1 has been amended to distinguish over Stefik. In particular, Stefik is silent on:

receiving from an electronic store, a hash value associated with the request to create the copy of previously received encrypted digital content;

SOM920000016US1

10

09/711,747

comparing the hash value received from the electronic store with a previously stored hash value corresponding to the previously received encrypted digital content;

updating the usage conditions associated with the previously received encrypted digital content to permit the at least one additional copy, in response to the hash value received from the electronic store matching the previously stored hash value; and

creating at least one additional copy onto a computer readable medium of the previously received encrypted digital content, if the at least one additional copy has been authorized in the usage conditions associated with the previously received encrypted digital content and without the need to re-receive the encrypted digital content being copied.

Accordingly, claim 1 of the present invention distinguishes over Stefik for at least these reasons.

The Examiner cites 35 U.S.C. § 102(b) and a proper rejection requires that a single reference teach (i.e., identically describe) each and every element of the rejected claims as being anticipated by Stefik.¹ The elements in independent claim 1 of "receiving from an electronic store, a hash value associated with the request to create the copy of previously received encrypted digital content;" as correctly noted by the Examiner on page 3, first paragraph of the Office Action is not taught or disclosed by Stefik. Accordingly, the present invention distinguishes over Stefik for at least this reason. The Applicants respectfully submit that the Examiner's rejection under 35 U.S.C. § 102(b) has been overcome.

¹ See MPEP §2131 (Emphasis Added) "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "The identical invention must be shown in as complete detail as is contained in the ... claim."

(4) Rejection under 35 U.S.C. §103(a) over Stefik in view of Yoshiura

As noted above, the Examiner rejected claims 2-16 under 35 U.S.C. § 103(a) as being unpatentable over Stefik (U.S. 5,715,403) in view of Yoshiura et al. (US 6,131,162). The Applicants have amended independent claims 1, 7, 9, and 15 to distinguish over Stefik taken alone and/or in view Yoshiura. As the Examiner correctly states on page 3, first paragraph of the Office Action "*Stefik does not disclose about: receiving from the electronic store a description of the previously received encrypted digital content required to be copied with an associated hash value*" and goes on to combine Stefik with Yoshiura.²

As an initial matter, Yoshiura is teaching hash values associated with digital signatures. The process of hashing to verify the authenticity of a message from a sender involves sending the hash value as part of the message digest. The receiver then computes a hash and compares it hash value generated for the message.³ See Yoshiura at col.2, lines 11-19. This is not the same as receiving a hash value from an electronic store and comparing the hash value to a previously stored hash value. Accordingly, independent claims 1, 7, 9, and 15 distinguish over Stefik taken alone and/or in view of Yoshiura for at least this reason.

Continuing further, the hash value sent from the electronic store is independent of the hash value previously stored. In contrast, in Yoshiura, the hash value used for digital signatures is sent along with the message; they are interdependent. The system in Yoshiura of digital signatures using hash values requires that the content (i.e. digital signature) be sent as part of the message in order to correctly calculate the hash value at the receiver. The Applicants submit that the combination of Stefik taken alone and/or

² Applicants make no statement whether such combination is even proper.

³ See www.whatis.com "*In addition to faster data retrieval, hashing is also used to encrypt and decrypt digital signatures (used to authenticate message senders and receivers). The digital signature is transformed with the hash function and then both the hashed value (known as a message-digest) and the signature are sent in separate transmissions to the receiver. Using the same hash function as the sender, the receiver derives a message-digest from the signature and compares it with the message-digest it also received. They should be the same.*"

in view of Yoshiura *teaches away* from "and without the need to re-receive the encrypted digital content being copied". Prior art that *teaches away* is per se demonstration of lack of *prima facie* obviousness.⁴ Yoshiura specifically *teaches* using hashing with digital signatures where the digital signature (i.e. content) is hashed at both the sender and at the receiver. In the present invention, the receiver uses a previously stored hash value which is provided by the sender. There is no need to calculate a hash value for the previously received encrypted content. Accordingly, independent claims 1, 7, 9, and 15 distinguish over Stefik taken alone and/or in view of Yoshiura for at least this reason as well.

Still, further both Stefik taken alone and/or in view of Yoshiura are completely silent on updating usage conditions associated with the content desired to be copied. Specifically, Stefik taken alone and/or in view of Yoshiura are completely silent on:

- claims 1, and 9

updating the usage conditions associated with the previously received encrypted digital content to permit the at least one additional copy, in response to the hash value received from the electronic store matching the previously stored hash value; and

- claims 7 and 15

determining if the first hash value received is identical to the second hash value and in response to the first hash and the second hash value being identical, then authorizing the creating additional copies onto at least one computer readable medium by updating the associated usage conditions and without the need to re-receive the encrypted digital content being copied.

Accordingly, Independent claims 1, 7, 9, and 15 distinguish over Stefik taken alone and/or in view of Yoshiura for at least this reason as well.

For the foregoing reasons, independent claims 1, 7, 9, and 15 as amended distinguish over Stefik taken alone and/or in view of Yoshiura. Claims 3-6, 8, 11-14, and 16 depend from independent claims 1, 7, 9, and 15 respectively, since dependent claims

⁴ See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)

contain all the limitations of the independent claims, claims 3-6, 8, 11-14, and 16 distinguish over Stefik taken alone and/or in view of Yoshiura, as well, and the Examiner's rejection should be withdrawn.

Newly added independent system claim 18 recites limitations similar to the limitations of method claim 1. Because independent claim 1 distinguishes over Stefik taken alone and/or in view of Yoshiura, claim 18 distinguishes as well. Moreover, since newly added claims 19-22 depend from claim 18, and since dependent claims contain all the limitations of the independent claims, claims 19-22 distinguish over Stefik taken alone and/or in view of Yoshiura, as well.

CONCLUSION

The remaining cited references have been reviewed and are not believed to effect the patentability of the claims as amended.

In this Response, Applicants have amended certain claims. In light of the Office Action, Applicants believe these amendments serve a useful clarification purpose, and are desirable for clarification purposes, independent of patentability. Accordingly, Applicants respectfully submit that the claim amendments do not limit the range of any permissible equivalents.

Applicants acknowledge the continuing duty of candor and good faith to disclosure of information known to be material to the examination of this application. In accordance with 37 CFR § 1.56, all such information is dutifully made of record. The foreseeable equivalents of any territory surrendered by amendment is limited to the territory taught by the information of record. No other territory afforded by the doctrine of equivalents is knowingly surrendered and everything else is unforeseeable at the time of this amendment by the Applicants and their attorneys.

Applicants respectfully submit that all of the grounds for rejection stated in the Examiner's Office Action have been overcome, and that all claims in the application are

SOM920000016US1

14


09/711,747

allowable. No new matter has been added. It is believed that the application is now in condition for allowance, which allowance is respectfully requested.

PLEASE CALL the undersigned if that would expedite the prosecution of this application.

Respectfully Submitted,

Date: January 3, 2005

By: 
Attorney for the Applicants
Jon A. Gibbons
(Reg. No. 37,333)

Customer Number 23334
Fleit, Kain, Gibbons, Gutman,
Bongini & Bianco P.L.
One Boca Commerce Center, Suite 111
551 N.W. 77th Street
Boca Raton, FL 33487
Telephone No.: (561) 989-9811
Facsimile No.: (561) 989-9812

SOM920000016US1

15

09/711,747